WE CLAIM:

1. A computer program product for controlling a computer to generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said computer program product comprising:

obtaining code operable to obtain from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and

generating code operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected.

2. A computer program product as claimed in claim 1, wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data.

3. A computer program product as claimed in claim 2, wherein said fixed location computing device is a user computer having communication link with said mobile computing device.

4. A computer program product as claimed in claim 2, wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronised.

5. A computer program product as claimed in claim 4, wherein said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronisation.

6. A computer program product as claimed in claim 4, when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware definition data stored on said mobile computing device and said fixed location computing device are compared, and, if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device.

7. A computer program product as claimed in claim 2, wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable.

8. A computer program product as claimed in claim 7, wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data.

9. A computer program product as claimed in claim 7, wherein said different types of mobile computing device correspond to different types of operating system computer program used by mobile computing devices.

10. A computer program product as claimed in claim 7, wherein said fixed location computer device detects to which mobile computing devices it may transfer computer files by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices.

11. A computer program product as claimed in claim 2, wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device.

12. A computer program product as claimed in claim 2, wherein said fixed location computing device checks for updated master malware definition data becoming available from said data source and, if such updated master malware definition data becomes available, then repeats said steps of obtaining, identifying and generating.

13. A computer program product as claimed in claim 11, wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

14. A computer program product as claimed in claim 2, wherein said master malware definition data is also used to protect said fixed location computing device from malware.

15. A computer program product as claimed in claim 2, wherein said fixed location computing device is connected to said data source by a fixed internet link.

16. A computer program product as claimed in claim 1, wherein said items of malware include one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

17. A method of generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said method comprising the steps of:

obtaining from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying one or more classes of malware threat against which said mobile computing device is to be protected; and

generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected.

18. A method as claimed in claim 17, wherein said steps of obtaining, identifying and generating are performed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data.

19. A method as claimed in claim 18, wherein said fixed location computing device is a user computer having communication link with said mobile computing device.

20. A method as claimed in claim 18, wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronised.

21. A method as claimed in claim 20, wherein said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronisation.

22. A method as claimed in claim 20, when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware definition data stored on said mobile computing device and said fixed location computing device are compared, and, if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware

definition data is transferred from said fixed location computing device to said mobile computing device.

23. A method as claimed in claim 18, wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable.

24. A method as claimed in claim 23, wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data.

25. A method as claimed in claim 23, wherein said different types of mobile computing device correspond to different types of operating system computer program used by mobile computing devices.

26. A method as claimed in claim 23, wherein said fixed location computer device detects to which mobile computing devices it may transfer computer files by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices.

27. A method as claimed in claim 18, wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device.

28. A method as claimed in claim 18, wherein said fixed location computing device checks for updated master malware definition data becoming available from said data source and, if such updated master malware definition data becomes available, then repeats said steps of obtaining, identifying and generating.

29. A method as claimed in claim 27, wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

30. A method as claimed in claim 18, wherein said master malware definition data is also used to protect said fixed location computing device from malware.

31. A method as claimed in claim 18, wherein said fixed location computing device is connected to said data source by a fixed internet link.

32. A method as claimed in claim 17, wherein said items of malware include one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

33. Apparatus for generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said apparatus comprising:

obtaining logic operable to obtain from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying logic operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and

generating logic operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected.

34. A computer program product as claimed in claim 33, wherein said obtaining logic, said identifying logic and said generating logic are provided by a fixed location computing device, said fixed location computer being operable to transfer to said

mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data.

35. A computer program product as claimed in claim 34, wherein said fixed location computing device is a user computer having communication link with said mobile computing device.

36. A computer program product as claimed in claim 34, wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronised.

37. A computer program product as claimed in claim 36, wherein said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronisation.

38. A computer program product as claimed in claim 36, when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware definition data stored on said mobile computing device and said fixed location computing device are compared, and, if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device.

39. A computer program product as claimed in claim 34, wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable.

40. A computer program product as claimed in claim 39, wherein user controlled policy data is used in combination with said threat data to control against which

classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data.

41. A computer program product as claimed in claim 39, wherein said different types of mobile computing device correspond to different types of operating system computer program used by mobile computing devices.

42. A computer program product as claimed in claim 39, wherein said fixed location computer device detects to which mobile computing devices it may transfer computer files by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices.

43. A computer program product as claimed in claim 34, wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device.

44. A computer program product as claimed in claim 34, wherein said fixed location computing device checks for updated master malware definition data becoming available from said data source and, if such updated master malware definition data becomes available, then repeats said steps of obtaining, identifying and generating.

45. A computer program product as claimed in claim 43, wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

46. A computer program product as claimed in claim 34, wherein said master malware definition data is also used to protect said fixed location computing device from malware.